DETAILED ACTION

1. This is in response to the amendment filed on 9 March 2010.

2. Claims 1-7, 9 and 10 are pending in the application.

3. Claims 1-7, 9 and 10 have been rejected.

4. Claim 8 has been cancelled.

Response to Arguments

5. Applicant's arguments with respect to claims 1-7, 9 and 10 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 2 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson U.S. Patent No. 6,990,591 B1 in view of Dowd et al U.S. Patent No. 7,315,801 B1 (hereinafter Dowd).

As to claim 1, Pearson discloses an intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network, the network intrusion detection system comprising:

Pearson discloses the intrusion detection system comprising means for monitoring activity relative to the computer system or network (i.e. Computer 102, LAN 104, and server 105 are typically connected to the Internet 108 through

a communication device 106 such as gateway, firewall, or other device that communicates data between one or more ports. According to an exemplary embodiment of the present invention, communication device 106 comprises a network firewall intrusion detection appliance that is further described with reference to FIG. 2 below. The firewall and intrusion detection functionality of communication device 106 protects the resources of LAN 104 from potential hackers, such as renegade users of the Internet 108 or unauthorized users of LAN 104, by monitoring the communications received into the device 106 and determining whether such communications comprise a security risk. The general operation of the firewall and intrusion detection functionality is described below with reference to FIG. 2.) [column 6, lines 5-20];

Pearson disclose means for receiving and storing one or more general rules. Pearson discloses that each of the general rules being representative of the effect on the computer system or network arising from plurality of specific instances of intrusion or attempted intrusion (i.e. In addition to firewall functionality, the preferred communication device 106 implements intrusion detection functionality via intrusion detector 160, by monitoring the communications received into communication device 106 and determining whether such communications comprise an attack or other security risk. More particularly, intrusion detector 160 inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list 170 of known attack signatures. Attack

signatures are activity patterns indicative of undesirable activity, i.e., evidence that an unauthorized communication has been received. Examples of attacks include Denial of Service (DoS) attacks, unauthorized access attacks, attempts to modify data or kill programs, protocol violations, and repeated access attempts indicating malicious intent. Representative examples of attack signatures are shown in FIG. 9 and will be further described below with reference to that figure. Intrusion detector 160 may also monitor for attacks by users that are authorized to be on LAN 104. Therefore, any attack or unauthorized activity on the network can be detected and the RMC 130 is automatically notified by an alert signal transmitted by the RMC communications module 165.) [column 8, lines 10-32].

Pearson discloses matching means for receiving data relating to activity relative to the computer system or network from the monitoring means and for comparing, in a semantic manner, sets of actions forming the activity against the one or more general rules to identify an intrusion or attempted intrusion (i.e. Method 700 begins at step 702, where an activated and remotely monitored communication device 106 receives a communication, for example from a hacker 150 (FIG. 1). This communication may constitute a threat or attack to the user's network, or may merely constitute a desired communication. Method 700 continues to step 704, where the received communication is compared to a list of known attacks and the result of the comparison is provided to a decision block 706. Preferably, all received communications are analyzed and compared to the list of known attacks. As described above with reference to FIG. 4B, a received

> communication will generally constitute a security risk if the type of communication received matches a communication type on the predetermined list 170 of communication types deemed to be attacks.) [column 16, lines 35-49].

Pearson does not teach that the matching means is done in a semantic manner and independently of the syntax of the activity.

Dowd teaches matching is done in a semantic manner and independently of the syntax of the activity. Dowd teaches simulating an attack on a network and for comparing it to a vulnerability database [column 4, lines 7-27].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson so that the matching means would have been done in a semantic manner and independently of the syntax of the activity. This would have been accomplished by simulating an attack on the network and comparing to a database of vulnerabilities.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson by the teaching of Dowd because it provides a system and method for analyzing the vulnerability of a network based on its current configuration by investigating possible attacks on a model of the network [column 1, lines 48-54].

As to claim 2, Pearson teaches that the one or more general rules forms a knowledge base of the system (i.e. The function of intrusion detection is well known to those skilled in the art. Typically, an intrusion detection function is carried out in software, and can be implemented in software, hardwire, or firmware. Typically, intrusion detection is carried out by comparing an

incoming communication (usually comprising a string of characters embedded within a TCP/IP packet, such characters being provided by another computer or a user of another computer that is requesting services) to a list of known attack signatures stored in an attack signature list 170. The attack signature list is preferably stored in a rewritable memory within the communication device 106 so that the list can be updated as new attack signatures are identified.) [column 8, lines 33-45].

As to claim 6, Pearson discloses an intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network, the intrusion detection system comprising:

> Pearson discloses the intrusion detection system comprising means for monitoring activity relative to the computer system or network (i.e. Computer 102, LAN 104, and server 105 are typically connected to the Internet 108 through a communication device 106 such as gateway, firewall, or other device that communicates data between one or more ports. According to an exemplary embodiment of the present invention, communication device 106 comprises a network firewall intrusion detection appliance that is further described with reference to FIG. 2 below. The firewall and intrusion detection functionality of communication device 106 protects the resources of LAN 104 from potential hackers, such as renegade users of the Internet 108 or unauthorized users of LAN 104, by monitoring the communications received into the device 106 and determining whether such communications comprise a security risk. The general

operation of the firewall and intrusion detection functionality is described below with reference to FIG. 2.) [column 6, lines 5-20].

Pearson discloses means for initially receiving and storing a knowledge base comprising one or more general rules. Pearson discloses that each of the general rules being representative of characteristics associated with a plurality of specific instances of intrusion or attempted intrusion (i.e. In addition to firewall functionality, the preferred communication device 106 implements intrusion detection functionality via intrusion detector 160, by monitoring the communications received into communication device 106 and determining whether such communications comprise an attack or other security risk. More particularly, intrusion detector 160 inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list 170 of known attack signatures. Attack signatures are activity patterns indicative of undesirable activity, i.e., evidence that an unauthorized communication has been received. Examples of attacks include Denial of Service (DoS) attacks, unauthorized access attacks, attempts to modify data or kill programs, protocol violations, and repeated access attempts indicating malicious intent. Representative examples of attack signatures are shown in FIG. 9 and will be further described below with reference to that figure. Intrusion detector 160 may also monitor for attacks by users that are authorized to be on LAN 104. Therefore, any attack or unauthorized activity on the network can

be detected and the RMC 130 is automatically notified by an alert signal transmitted by the RMC communications module 165.) [column 8, lines 10-32].

Pearson discloses means for automatically generating and storing in the knowledge base (i.e. Method 700 begins at step 702, where an activated and remotely monitored communication device 106 receives a communication, for example from a hacker 150 (FIG. 1). This communication may constitute a threat or attack to the user's network, or may merely constitute a desired communication. Method 700 continues to step 704, where the received communication is compared to a list of known attacks and the result of the comparison is provided to a decision block 706. Preferably, all received communications are analyzed and compared to the list of known attacks. As described above with reference to FIG. 4B, a received communication will generally constitute a security risk if the type of communication received matches a communication type on the predetermined list 170 of communication types deemed to be attacks.) [column 16, lines 35-49].

Pearson does not teach that the matching means is done in a semantic manner and independently of the syntax of the activity.

Dowd teaches matching is done in a semantic manner and independently of the syntax of the activity. Dowd teaches simulating an attack on a network and for comparing it to a vulnerability database [column 4, lines 7-27].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson so that the matching means would have

been done in a semantic manner and independently of the syntax of the activity. This would have been accomplished by simulating an attack on the network and comparing to a database of vulnerabilities.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson by the teaching of Dowd because it provides a system and method for analyzing the vulnerability of a network based on its current configuration by investigating possible attacks on a model of the network [column 1, lines 48-54].

7. Claims 3-5, 7, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson U.S. Patent No. 6,990,591 B1 and Dowd et al U.S. Patent No. 7,315,801 B1 (hereinafter Dowd) as applied to claim 1 above, and further in view of "Applications of Inductive Logic Programming" (hereinafter Bratko).

As to claim 3, the Pearson-Dowd combination discloses if no session entry is found in step 102, a new session entry is created in the session cache 44 in step 106. Session data, which includes any matches identified by executing attack signature profile instructions on a data packet, are entered into the new session entry in step 108 and the session entry is entered into the state cache 44 in step 110 [Pearson column 9, lines 21-27].

The Pearson-Dowd combination does not teach that the means for automatically generating and storing a new general rule (i.e. new session entry) comprises inductive logic programming means.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples.

Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Pearson-Dowd combination so that the means for generating and storing a new rule (i.e. updated rules) would have been done by using inductive logic programming.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Pearson-Dowd combination by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

As to claims 4, 9 and 10, the Pearson-Dowd combination discloses that in step 56 the communication module 30 of the data repository 12 distributes the signature profiles to the various data collectors 10 throughout the network. Upon receiving a set or sets of attack signature profiles, each data collector 10 stores the set or sets of profiles it receives from the data repository 12 in its signature profile memory 39 [Pearson column 6, lines 50-56].

The Pearson-Dowd combination does not teach that the one or more general rules is or are represented in a logic programming language.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Pearson-Dowd combination so that the rules as taught would have been represented by inductive logic programming.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Pearson-Dowd combination by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

As to claim 5, the Pearson-Dowd combination discloses that multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions [Pearson column 5, lines 26].

The Pearson-Dowd combination does not teach that inductive logic programming techniques are applied by the system to an attack an intrusion or attempted intrusion.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples.

Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Pearson-Dowd combination so that the rules of an attack would have been applied by inductive logic programming to derive positive examples.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Pearson-Dowd combination by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

As to claim 7, Pearson discloses an intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network, the intrusion detection system comprising:

> Pearson discloses the intrusion detection system comprising means for monitoring activity relative to the computer system or network (i.e. Computer 102, LAN 104, and server 105 are typically connected to the Internet 108 through a communication device 106 such as gateway, firewall, or other device that communicates data between one or more ports. According to an exemplary

embodiment of the present invention, communication device 106 comprises a network firewall intrusion detection appliance that is further described with reference to FIG. 2 below. The firewall and intrusion detection functionality of communication device 106 protects the resources of LAN 104 from potential hackers, such as renegade users of the Internet 108 or unauthorized users of LAN 104, by monitoring the communications received into the device 106 and determining whether such communications comprise a security risk. The general operation of the firewall and intrusion detection functionality is described below with reference to FIG. 2.) [column 6, lines 5-20].

Pearson discloses means for initially receiving and storing in a knowledge base data representative of the effect on the computer system or network arising from one or more specific instances or classes of intrusion or attempted intrusion. (i.e. In addition to firewall functionality, the preferred communication device 106 implements intrusion detection functionality via intrusion detector 160, by monitoring the communications received into communication device 106 and determining whether such communications comprise an attack or other security risk. More particularly, intrusion detector 160 inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list 170 of known attack signatures. Attack signatures are activity patterns indicative of undesirable activity, i.e., evidence that an unauthorized communication has been received. Examples of attacks include Denial of Service (DoS) attacks, unauthorized access

attacks, attempts to modify data or kill programs, protocol violations, and repeated access attempts indicating malicious intent. Representative examples of attack signatures are shown in FIG. 9 and will be further described below with reference to that figure. Intrusion detector 160 may also monitor for attacks by users that are authorized to be on LAN 104. Therefore, any attack or unauthorized activity on the network can be detected and the RMC 130 is automatically notified by an alert signal transmitted by the RMC communications module 165.) [column 8, lines 10-32].

Pearson discloses matching means for receiving data relating to activity relative to the computer system or network from the monitoring means and for comparing sets of actions forming the activity against the stored data to identify an intrusion or attempted intrusion (i.e. Method 700 begins at step 702, where an activated and remotely monitored communication device 106 receives a communication, for example from a hacker 150 (FIG. 1). This communication may constitute a threat or attack to the user's network, or may merely constitute a desired communication. Method 700 continues to step 704, where the received communication is compared to a list of known attacks and the result of the comparison is provided to a decision block 706. Preferably, all received communications are analyzed and compared to the list of known attacks. As described above with reference to FIG. 4B, a received communication will generally constitute a security risk if the type of communication received matches

a communication type on the predetermined list 170 of communication types deemed to be attacks.) [column 16, lines 35-49].

Pearson does not teach that the updating means include inductive logic programming means for updating the stored data to take into account the effect on the computer system or network arising from further instances or classes of intrusion or attempted intrusion occurring after the knowledge base has been initially received and stored. Pearson does not teach that the matching means is done in a semantic manner and independently of the syntax of the activity.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66]. Dowd teaches matching is done in a semantic manner and independently of the syntax of the activity. Dowd teaches simulating an attack on a network and for comparing it to a vulnerability database [column 4, lines 7-27].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson so that the updating means of the rules would have been done using inductive logic programming. The matching means would have been done in a semantic manner and independently of the syntax of the activity. This would have been accomplished by simulating an attack on the network and comparing to a database of vulnerabilities.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson by the teaching of Wrobel because one of the

main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66]. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson by the teaching of Dowd because it provides a system and method for analyzing the vulnerability of a network based on its current configuration by investigating possible attacks on a model of the network [column 1, lines 48-54].

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431